

Serial No. 09/710,541
Atty Dkt: 99-956

REMARKS

This Reply is responsive to the non-final Office Action¹ of October 5, 2005. Claims 1-32 were presented for examination and were rejected. No claims are added or canceled; claims 1-32 are pending. Claims 1, 12, 19, 24 and 32 are independent claims.

Claims 1-31 are rejected under 35 U.S.C. §103(a) as being un-patentable over Aura, U.S. Patent No. 6,711,400 B1 (referred to hereinafter as "Aura") in view of Raith, U.S. Patent No. 5,241,598. Claim 32 is rejected under 35 U.S.C. §103(a) as being un-patentable over Aura in view of Raith and further in view of Maupin, U.S. Patent No. 6,600,917 (referred to hereinafter as "Maupin"). Applicant respectfully traverses these rejections because Aura has admitted deficiencies and newly-cited Raith does not cure those deficiencies. Maupin, likewise, does not cure those deficiencies. Consider, e.g., claim 1:

A method for use in authenticating a service network to a station, the station having a home environment network, the method comprising: storing a key at the service network; transmitting information to the station from the service network that enables the station to compute the key stored at the service network; receiving a request for service at the service network from the station; adjusting a verification value at each usage of the key; and transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network. (Emphasis added.)

There are three separate entities recited in claim 1: "a service network" which is the visited network, or the network into which the user/subscriber of, e.g., a cell phone, has roamed; "a station", which is the mobile station or, e.g., a cell phone; and "a home

¹ The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicant may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicant does not automatically subscribe to, or acquiesce in, any such statement. Further, silence with regard to rejection of a dependent claim, when such claim depends, directly or indirectly, from an independent claim which Applicant deems allowable for reasons provided herein, is not acquiescence to such rejection of that dependent claim, but is recognition by Applicant that such previously lodged rejection is moot based on remarks and/or amendments presented herein relative to that independent claim.

Serial No. 09/710,541
Atty Dkt: 99-956

environment network” which is the home network for that subscriber/user from which the subscriber can roam into a service network. Claim 1 clearly calls for storing the “key” in one of those entities, namely the service network, i.e., storing the key in the visited network.

The Office Action, pages 3-4, associates a number of sections in Aura with various claim elements of claim 1, with which Applicant does not necessarily agree. However, Applicant does agree with the Office Action page 4 where it indicates that Aura does not expressly disclose adjusting a verification value at each usage of the key and does not expressly disclose transmitting, from the service network to the station, information corresponding to the verification value. The Office Action relies on Raith for these admitted deficiencies in Aura.

In the Office Action, pages 4-5, it states: “Raith discloses the use of a counter in association with the usage of an encryption key by a mobile station (see for example, col. 8, lines 54-67; col. 21, line 22-col. 22, line 37, where incrementing the counter each time the rolling key is updated is functionally equivalent to the adjusting a verification value at each usage of the key).” (Emphasis added.) Applicant respectfully disagrees.

To begin with, the column 8, lines 54-67 section of Raith discusses a method and system for “resynchronization of a rolling key.” Synchronization is a problem mentioned in Raith, at least in column 7, lines 3-20: “The rolling key or B-key used to counteract false mobile stations in the network may occasionally fall out of synchronization.” (col. 7, lines 3-5) “The valid mobile station will then appear to the network as a fraudulent mobile station.” (col. 7, lines 10-11) Thus, the counter value in the column 8, lines 54-67 section to which the Office Action refers is merely indicative of the number of times the rolling key has been updated for synchronization purposes. This has nothing to do with “adjusting a verification value at each usage of the key” as recited in claim 1.

In the next section to which the Office Action refers, column 21, line 22, to column 22, line 37, all of the discussion relating to “Call Counter” relates merely to tracking the number of calls to and from the mobile station for the purpose of monitoring

Serial No. 09/710,541
Atty Dkt: 99-956

fraudulent use of network services, and is quite different from the claimed authenticating method aimed at preventing or controlling that fraud in the first place. In this section there is no substantive discussion of a key and merely tracking a number of calls has nothing to do with “adjusting a verification value at each usage of the key” as recited in claim 1. In the remaining “B-key Index” portion of this section to which the Office Action refers, all of the discussion refers to a counter which is incremented every time the network and mobile station update the rolling key. As discussed below, the rolling key is quite different from Applicant’s recited key in at least one important respect, wherefore incrementing a counter in Raith every time this non-equivalent key is updated is not anticipatory or suggestive of Applicant’s recited “adjusting” step.

According to Raith, its rolling key and B-key may be the same thing (*see: e.g., column 6, lines 54-55; column 7, line 3; column 18, line 23; column 19, line 17*). As noted above, the Office Action takes the position that “incrementing the counter each time the rolling key is updated is functionally equivalent to adjusting a verification value at each usage of the key.” (Office Action, pages 4-5) Thus, based on Raith, if the counter would be incremented each time the rolling key is updated, then it appears that the counter would be incremented each time the B-key is updated. But, either the B-key or the rolling key are not equivalent to Applicant’s recited “key” of claim 1.

Claim 1 calls for “storing a key at the service network” (at the visited network). But, quite differently, Raith stores its B-key and/or its rolling key at the home network and/or in the mobile station’s semi-permanent memory! Indeed, there is no storage in Raith of the rolling key or the B-key in the service network (visited network).

It should be noted, however, that inter-network communications are simplified and security is enhanced if the secret keys, e.g., the A-key (and the B-key), are stored in the home network, or at least in a location under the control of the home network, so that only security variables, e.g., S-key, are transmitted between the home network and a visited network. In parts of the remaining discussion, it is assumed that the secret keys are stored in, or controlled by, the home network of the mobile station. (Raith, Column 16, lines 53-63, Emphasis added.)

Serial No. 09/710,541
Atty Dkt: 99-956

The authentication system of FIG. 4 provides an anti-cloning safeguard based on a dynamic, i.e., changeable, "rolling key" which is stored in each of the home network and the mobile station and which is used along with the permanent secret key (A-key) for calculating authentication responses, temporary encryption keys and new rolling keys. (Raith, Column 18, lines 5-11, Emphasis added.)

(3) "B-key.sub.s`p " is the stored value of the B-key in the mobile station's semi-permanent security and identification memory. B-key.sub.s-p is used as the B-key input to AUTH and is temporarily replaced by the selected value, for example, a fixed value, when the network signals a B-key reset.

(4) "B'-key.sub.s " is the stored value of the previously used B-key.sub.s-p in the mobile station's temporary memory.

(5) "BKEYI.sub.s-p " is the stored value of the B-key index in the mobile station's semi-permanent security and identification memory. BKEYI.sub.s-p is incremented whenever the mobile station steps (updates) the B-key.sub.s-p. (Raith, column 34, lines 22-34, Emphasis added.)

Clearly, Raith teaches, as exemplified by the above sections, that its rolling key or B-key is stored in its home network or in its mobile station or both, but not in its visited network. The Office Action relies on Raith to show "adjusting a verification value at each usage of the key" (claim 1, emphasis added) but Applicant's recited key is one which has been stored in the service network, i.e., the visited network. (See claim 1 limitation: "storing a key at the service network.") Thus, Raith's rolling key or B-key, being stored in other than the service network is other than Applicant's recited key². Therefore, Raith does not show "adjusting a verification value at each usage of the key" as recited in claim 1 since it shows a different key from the claimed key.

In addition to not teaching Applicant's recited "adjusting" step, as a result of Raith not showing Applicant's recited key, the recited "transmitting" step is also not shown in Raith for the following reasons: (1) claim 1 calls for transmitting, from the

² There is a key which is stored in Raith's visited network, namely the "S-key": "The visited network stores the new S-key for use in future calls involving the visiting mobile station." (Raith, column 23, lines 42-44). However, the S-key is merely a security variable according to the first Raith section quoted above and is not a secret key. It is a short-term encryption key used for a limited period of time; it does not map to Applicant's recited key. (Raith, col. 17, lines 37-58)

Serial No. 09/710,541
Atty Dkt: 99-956

service network to the station, information corresponding to the verification value; and (2) claim 1 calls for the verification value to be adjusted at each usage of the key (the recited key); and (3) the recited key is not disclosed or suggested in Raith; wherefore (4) information corresponding to an adjusted verification value based on usage of an equivalent to Applicant's recited key is not disclosed by Raith and therefore cannot be transmitted in Raith. Thus, Raith does not show "transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network" as recited in claim 1.

In accordance with MPEP 2143, to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure. And, all three of these basic criteria must be met - if any one is not met the prima facie case of obviousness is not made.

In this instance, the prior art references Aura and Raith, taken alone or in combination, do not teach or suggest all limitations of claim 1 for the reasons given above. Aura does not disclose or suggest adjusting a verification value at each usage of the key and does not disclose or suggest transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network, per the Examiner's admission. Raith does not disclose or suggest adjusting a verification value at each usage of the key and does not disclose or suggest transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network,

Serial No. 09/710,541
Atty Dkt: 99-956

per the above analysis. Accordingly a prima facie case of obviousness has not been established against claim 1 on this basis alone.

Furthermore, neither Aura or Raith provide support for any motivation to combine the references. Merely because Aura relates to cellular communication authentication (title) and because Raith may relate to a similar subject of cellular communication verification and validation (title) does not, by itself, manifest any motivation in either reference to combine itself with the other reference. Since Aura does not disclose counters (the terms "count" or "counter" do not appear in Aura), it cannot disclose their desirability in this context and therefore cannot disclose a motivation to seek a counter augmentation to enhance its performance.

With respect to Raith, to support combinability of Raith with Aura, the Office Action, page 5, first points to Raith, column 19, lines 7-14. This section merely discusses prevention of a fraudulent mobile station from gaining access to the network, but this does not suggest combining Raith with Aura, much less combining its counter with Aura. The Office Action also points to Raith, column 6, lines 57-67, which merely discusses a two-way authentication procedure to enhance security to meet the threat of a false base station, but this again does not suggest combining Raith with Aura, much less combining its counter with Aura. Applicant submits that any motivation for combining these references is solely derived from impermissible hindsight, i.e., only after reviewing Applicant's disclosure and claims and appreciating the advantages provided thereby. Accordingly a prima facie case of obviousness has not been established against claim 1 on this second, additional basis alone.

For any or all of the reasons given above, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of claim 1 should be withdrawn and the claim allowed.

Independent claim 12 recites, *inter alia*: "computing a key based on the information transmitted from the service network to the station, the computed key also being stored by the service network; maintaining an indicator of key usage at the station; transmitting, from the service network to the station, an indicator of key usage maintained by the service network; and comparing the key usage indicator maintained by

Serial No. 09/710,541
Atty Dkt: 99-956

the service network with the key usage indicator maintained by the station enabling the station to authenticate the service network” The “computed key” in claim 12 is stored in the service network (the visited network) as in claim 1, and an indicator of “key usage” in claim 12 is equivalent to each “usage of the key” recited in claim 1. The “transmitting” and “comparing” steps of claim 12 are generally comparable with the “transmitting” step of claim 1. Therefore, for reasons similar to those given above with respect to claim 1, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of claim 12 should be withdrawn and the claim allowed.

Independent claim 19 recites, *inter alia*: “storing a key at the service network” and “adjusting a verification value at each usage of the key; transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network” which is identical language to that of claim 1. For reasons given above with respect to claim 1, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of claim 19 should be withdrawn and the claim allowed.

Independent claim 24 recites, *inter alia*: “storing a key at the service network” and “adjusting a verification value at each usage of the key; and transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network” which is identical language to that of claim 1. For reasons given above with respect to claim 1, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of claim 24 should be withdrawn and the claim allowed.

Independent claim 32 recites, *inter alia*: “storing the SSK at the service network” and “adjusting a verification value at each usage of the SSK; and transmitting, from the service network to the station, information corresponding to the verification value that forms a part of a verification computation enabling the station to authenticate the service network” which is very similar language to that of claim 1. Maupin does not cure the deficiencies of Aura or Raith. For reasons given above with respect to claim 1, it is

Serial No. 09/710,541
Atty Dkt: 99-956

respectfully submitted that the 35 U.S.C. § 103(a) rejection of claim 32 should be withdrawn and the claim allowed.

Furthermore, all dependent claims, namely 2-11, dependent from independent claim 1, 13-18 dependent from independent claim 12, 20-23 dependent from independent claim 19, and 25-31 dependent from independent claim 24 are likewise allowable at least for reasons based on their dependencies from allowable independent base claims. In addition, dependent claims are allowable for reasons based on their individual recitations.

Serial No. 09/710,541
Atty Dkt: 99-956

CONCLUSION


Reconsideration and allowance are respectfully requested based on the above amendments and remarks. It is respectfully submitted that all claims and, therefore, this application are in condition for allowance.

If there are any remaining issues or if the Examiner believes that a telephone conversation with Applicant's attorney would be helpful in expediting the prosecution of this application, the Examiner is invited to call the undersigned at (972) 718-4800.

To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged to deposit account number 07-2347. Please charge any other fees due, or credit any overpayment made to that account.

Respectfully submitted,

Date: December 29, 2005


Joel Wall

Attorney for Applicant

Registration No. 25,648

Verizon Corporate Services Group Inc.
c/o Christian Andersen
600 Hidden Ridge, HQE03H14
Irving, TX 75038
Tel: (972) 718-4800
CUSTOMER NO. 32127